Job Opportunity

State Controller's Office

Position:	Senior Information Systems Analyst (Specialist)	Statewide

Location: Information Security Office
300 Capitol Mall, Suite #1510, Sacramento, CA 95814

Issue Date: September 6, 2006

Final Filing Date: Until Filled

Contact/Telephone:
Information Security Office, 916-445-1720

Who May Apply: Individuals who are currently in this classification, eligible for lateral transfer or promotion, or reachable on a certification list.

California Relay Service: 1-800-735-2929

Position Number(s): 051-726-1337-001

Please call (916)323-3055 to request reasonable accommodations

Scope of the Position:

Under general supervision provided by the Data Processing Manager III, the Senior ISA acts as a lead analyst in the administration of the Information Security program for the State Controller's Office by effectively applying the principles and practices of information security. The Senior ISA provides technical expertise and leadership to the ISO team; performs the more complex security technical analysis, design, and problem resolutions; and oversees the Business Continuity, Disaster Recovery, and Operational Recovery programs. Possess familiarity and understanding of government regulations and administration procedures regarding Information Security, Physical Security, Risk Management Planning, and Information Technology. Applies security industry best practices on projects and researches trends to provide recommendations of optimum solutions. Acts on behalf of the Chief ISO by performing those duties and functions when required.

Duties and Responsibilities:

Candidates must perform the following essential functions with or without reasonable accommodations

The Senior Information Systems Analyst must possess a sound technical background, strong motivation, and be able to function as the lead technical analyst performing specific duties which include but are not limited to the following:

- Execute a high level of competency in the major areas of IT Security (confidentiality, integrity, and availability) including data security, physical security, and business continuity.
- Establish and maintain internal/external relations, becoming the key resource contact for the Information Security Office in the areas of security policy, security awareness, and incident response.
- Provide risk analysis and assessments for systems and projects, and provide findings in a written format to the CISO for consideration.
- Provide security consultation in the development of bid proposals for procurement efforts.

The State Controller's Office is committed to providing equal opportunity to all regardless of race, color, creed, national origin, ancestry, sex, marital status, gender, disability, religious or political affiliation, age, or sexual orientation.

- Develop requirements and design specifications for Security Risk Management processes.
- Develop, maintain and implement the SCO Business Continuity Program (including Disaster Recovery, Business Resumption, and Communications). Provide cross-training and ensure sustainability of this plan.
- Assist the ISO staff in the development of new security practices.
- Initiate security improvements in existing projects and processes.
- Evaluate long- and short-term solutions to complex information systems security protocols and/or procedures.
- Participate in the more complex problem resolutions for mainframe and LAN/WAN environments.
- Develop, maintain, and implement a Security Incident Response program.
- Assist the CISO with budget processes, hiring of new staff, and legislative analysis.
- Maintain a high level of expertise and knowledge in SCO projects and services.
- Be proactive in identifying issues, develop solution recommendations, and present to management.
- Interact with SCO technical teams to build security awareness, trust, and support.
- Interact in a positive and productive manner with all individuals and groups internal and external to the ISO.
- Gain and maintain familiarity with RACF help desk functions and assist in workflow monitoring.
- Review information security contract language for CIRM and SOW documents; provide recommendations on language changes if needed.
- Participate as a secondary contact for the site security alarm response.

DESIRABLE QUALIFICATIONS:

Attributes:

- IT Security principles and practices including ISO 17799, NIST and FISMA.
- Possess a security certification such as CISSP or SANS GIAC.
- Business Continuity principles and practices.
- Business Continuity certified; such as ABCP or CBCP.
- Leadership in a technical environment.
- Ability to reason logically and communicate effectively.
- Experience and ability to work independently.
- Skills in meeting facilitation and public speaking.
- Work well with others and contribute to a positive teamwork environment.
- Ability to perform comprehensive analyses of security risks.
- Possess effective communication skills.

Desired Experience and Knowledge:

- Completed Staff Work.
- Project Management.
- Prior work experience in the IT Security or equivalent industry.

Reasons Why You Should Consider Working in the Information Security Office:

- An opportunity to participate in and contribute to a highly visible and business critical industry
- Participation in an energetic team environment consisting of committed security professionals while gaining valuable experience applicable and marketable worldwide.

Applications will be screened and only the most qualified will be interviewed

How to Apply:

All hires will be subject to a background check.

For permanent positions, SROA and Surplus candidates should attach "surplus letters" to their application. Failure to do so may result in your application not being considered.

Please submit a STD. 678 State Application and Résumé to:

State Controller's Office
Information Security Office
300 Capitol Mall, Suite #1510
Sacramento, CA 95814

Attn: Chief Information Security Officer

Please reference position number on application.